

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE**

UNITED STATES OF AMERICA)	
Plaintiff,)	
)	
v.)	Case No.3:08-cr-175
)	JUDGES PHILLIPS/SHIRLEY
CLARK ALAN ROBERTS, and)	
SEAN EDWARD HOWLEY,)	
Defendants.)	

OBJECTIONS TO REPORT AND RECOMMENDATION [DOC. 88]

Comes the defendant, CLARK ALAN ROBERTS, by and through counsel and pursuant to the provisions of 28 U.S.C. § 636, and herein respectfully objects to the Report and Recommendation of the Magistrate Judge [Doc. 88]¹ which recommends that this Court deny his motion to suppress [Docs. 39 (motion), 40 (memorandum), and 61 (reply)].

I. FACTUAL BACKGROUND OF MOTION TO SUPPRESS AND OBJECTIONS.

The Report and Recommendation devotes several pages to an overview of the proof presented at the evidentiary hearing. [Doc. 88, pgs. 3-7].² The Court informed that “[a]ll other factual findings will be made as a part of the analysis of the issues,” [Doc. 88. Pg. 8], and Mr. Roberts will therefore address specific objections to the court’s findings by issue.

As an initial matter, though, Mr. Roberts would like to highlight certain facts and matters of proof that were not included in the court’s summary but which are relevant to Mr. Roberts’

¹ The Report and Recommendation was entered on December 21, 2009 [Doc. 88]. These objections are timely filed pursuant to Fed. R. Crim. Proc. 59(b)(2) (as amended) (requiring objections to be filed within 14 days after service of recommended disposition).

² Two and one-half pages of the Report and Recommendation relate to the testimony of Special Agent Kevin Gounaud of the F.B.I., whose testimony was elicited in response to the motions to suppress filed by Mr. Howley. [Doc. 88, pgs. 3-6].

argument that the search warrant lacked particularity on its face. See [Doc. 61, pg. 10]. Namely, in addition to the testimony of two witnesses at the suppression hearing, several exhibits were entered into evidence. See [Doc. 79] (listing, in part, the following exhibits: EXHIBIT 2 (Handwritten copy of receipt for Property Received/Returned/Released/Seized); EXHIBIT 2A (Typed copy of Exhibit 2); EXHIBIT 3 (SEALED Application & Affidavit for Search Warrant (21 pgs.) with Attachment A (2 pgs.) and Attachment B (2 pgs.)); EXHIBIT 4 (Search Warrant with 2 Attachments)).

As summarized in the Report and Recommendation, Attachment B to the search warrant listed the categories of items authorized to be seized. [Doc. 88, pgs. 15-16] (focusing on paragraphs three (3) through seven (7) of Attachment B). The handwritten inventory, by comparison, reflects what was actually taken pursuant to the search warrant, and three of its four pages catalog the photographs, e-mails, work orders, reports, miscellaneous documents, folders, files, binders, notes, drawings, diagrams, planners, timecards, and other items that were seized from various rooms, desks, and filing cabinets at Wyko. A fourth page is entirely devoted to listing the seven laptop and server hard drives seized, though it does not indicate the basis for concluding that these seven hard drives contained “evidence” of trade secret violations.

As stated on the record at the suppression hearing, the remedy requested by Mr. Roberts is to suppress any files that were contained on his laptop, including e-mails, and to suppress any files located on the server that pertain to his e-mails or backup files from his laptop as well as any portions of the server over which Mr. Roberts either had exclusive control or control greater than general employees within the company would have had. [Tr., pg. 41]. Mr. Roberts has standing to challenge the constitutionality of the seizure of these items; in addition, because the scope of the search pursuant to the warrant exceeded the authority granted by the issuing

magistrate, Mr. Roberts has also requested the suppression of all items seized from Wyko. The doctrine of severance sometimes permits courts to suppress only the evidence seized pursuant to the invalid portions of a warrant while admitting evidence seized based on any valid, separable parts of the warrant, see United States v. Ford, 184 F.3d 566, 579 (6th Cir. 1999), but when the lack of particularity is characteristic of the entire warrant, the suppression of all seized materials is the proper remedy. See United States v. Cioffi, No. 08-CR-415, 2009 WL 3738314, *9 and n.8 (E.D.N.Y. Nov. 2, 2009) (“Here the lack of particularity pervades the entire Warrant; there is, therefore, no valid portion under which the November 23rd Email could have been seized.”) (citing United States v. Matias, 836 F.2d 744 (2d Cir.1988), and United States v. George, 975 F.2d 72, 79 (2d Cir.1992)).

II. MR. ROBERTS HAS STANDING TO CHALLENGE THE SEARCH WARRANT AND THE SEARCH.

As summarized in the Report and Recommendation, Mr. Roberts “contend[s] that [his] rights under the Fourth Amendment were violated by both the issuance of the September 2007 search warrant authorizing the search of Wyko” and the manner of its execution. [Doc. 88, pg. 8]. The remedy for this violation is exclusion of evidence obtained in violation of the Fourth Amendment. The government responded to the motion to suppress and argued that Mr. Roberts lacked standing to challenge the warrant and search, suggesting that he lacked a legitimate expectation of privacy in what it characterized as the property of his employer. [Doc. 88, pg. 9]. The Report and Recommendation assessed the reasonableness of Mr. Roberts’ asserted privacy interests “by looking to (1) the defendant’s interest in and control of the place searched, (2) any measures the defendant took to ensure privacy, and (3) whether society recognizes the defendant’s expectation as reasonable.” [Doc. 88, pg. 12].

The court correctly found that Mr. Roberts “has a legitimate expectation of privacy in anything seized from his office and all of the files on his laptop computer.” [Doc. 88, pg. 11]. However, when addressing whether there was standing to challenge the seizure and search of information contained on Wyko’s server, the Report and Recommendation too narrowly interprets the recognized privacy interests which are granted to individuals in Mr. Roberts’ position (Director of Engineering) and which are associated with the types documents seized pursuant to the warrant (e.g., e-mail), and too heavily relies on the concept of control.

As such, Mr. Roberts specifically objects to the finding in the Report and Recommendation that Mr. Roberts only has standing to challenge the search of his office, his individual work computer, and the seizure of his “own, password protected files on the server, if any existed.” [Doc. 88, pg. 14]. More specifically, Mr. Roberts objects to the court’s finding that he “could not be secure in the privacy of [his] email and other similarly situated files on the server.” [Doc. 88, pg. 13]. As he set forth in Mr. Roberts’ motion to suppress, “[i]t has long been held that one has standing to object to a search of his office.” See [Doc. 61, pg. 3] (quoting Mancusi v. DeForte, 392 U.S. 364, 369-70 (1968)). There can be a privacy interest in the content of a communication apart from the information used to address the message. See Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) cert. granted, City of Ontario v. Quon, No. 08-1472, 2009 WL 1513112 (U.S. Dec. 14, 2009).

As set forth in Mr. Roberts’ memorandum in support of his motion to suppress, in Mancusi v. DeForte, 392 U.S. 364 (1968), in a situation analogous to the shared server in this case, the defendant objected to the search of an office he shared with several other workers. The Supreme Court, characterizing the issue as whether the defendant had an expectation of privacy in the area, reasoned:

The record reveals that the office where DeForte worked consisted of one large room, which he shared with several other union officials. The record does not show from what part of the office the records were taken, and DeForte does not claim that it was a part reserved for his exclusive personal use. The parties have stipulated that DeForte spent ‘a considerable amount of time’ in the office, and that he had custody of the papers at the moment of their seizure.

We hold that in these circumstances DeForte had Fourth Amendment standing to object to the admission of the papers at his trial. It has long been settled that one has standing to object to a search of his office, as well as of his home. . . . **It seems to us that the situation was not fundamentally changed because DeForte shared an office with other union officers. DeForte still could reasonably have expected that only those persons and their personal or business guests would enter the office, and that records would not be touched except with their permission or that of union higher-ups.** This expectation was inevitably defeated by the entrance of state officials, their conduct of a general search, and their removal of records which were in DeForte's custody. It is, of course, irrelevant that the Union or some of its officials might validly have consented to a search of the area where the records were kept, regardless of DeForte's wishes, for it is not claimed that any such consent was given, either expressly or by implication.

Mancusi v. DeForte, 392 U.S. 364, 369-70 (1968) (internal citations omitted) (emphasis added).

See also [Doc. 61, pg. 3] (citing United States v. Mancini, 8 F.3d 104 (1st Cir. 1993); Villano v. United States, 310 F.2d 680 (10th Cir. 1962); United States v. Lefkowitz, 464 F.Supp. 227 (C.D. Cal. 1979)). Mr. Roberts also cited cases in which standing was more likely to be found because the seized item was connected with the defendant or because the defendant played a key role in creating the item. See [Doc. 61, pg. 4] (citing United States v. Anderson, 154 F.3d 1225 (10th Cir. 1998); United States v. Alwelt, 532 F.2d 1165 (7th Cir. 1976)).

Whereas the Report and Recommendation correctly found that “the defendants’ expectation of privacy in some information that they stored on the server, especially those files that were password protected, was an interest that society would recognize,” it limited the realm

of recognized privacy and found that Mr. Roberts lacked standing to challenge the search of files other than his own password protected files. [Doc. 88, pg. 13-14]. The “other files” in which the Report and Recommendation claims Mr. Roberts has no cognizable privacy interest include his e-mail, because, as summarized by the Court:

Defendant Roberts agreed that email was out of his control once he sent it. The Court notes that the system would likely back up an email from the defendants’ computers but also from their in-house recipients’ computers. Thus, numerous copies of any given email exist on the server. The Court finds that the defendants could not be secure in the privacy of their email and other similarly situated files on the server. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (observing that the sender “would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient”). But c.f. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906 (9th Cir. 2008) (holding that sender and recipients may have a reasonable expectation of privacy in the contents of text messages sent from a pager provided by the sender’s employer) cert. granted, City of Ontario v. Quon, No. 08-1472, 2009 WL 1513112 (U.S. Dec. 14, 2009).

[Doc. 88, pg. 13]. Whether the content of e-mail exists in multiple, backed-up copies or was sent to several recipients does not lessen an individual’s privacy interest in the content of his messages for Fourth Amendment purposes. Compare [Doc. 88, pg. 13-14] (“The Court finds that the defendants could not be secure in the privacy of their email and other similarly situated files on the server. . . . [T]he Court finds that the defendants had no reasonable expectation of privacy in data on the server other than their own files that were password protected.”) with United States v. Cioffi, No. 08-CR-415, 2009 WL 3738314 (E.D.N.Y. Nov. 2, 2009),³ Brown-Criscuolo

³ “One preliminary matter is *not* in question: The government does not dispute that Tannin had a reasonable expectation of privacy in the contents of his personal email account. See United States v. Zavala, 541 F.3d 562, 577 (5th Cir.2008) (“[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. [The defendant] had a reasonable expectation of privacy regarding this information.”); United States v. Forrester, 512 F.3d 500, 511 (9th Cir.2008) (“E-mail, like physical mail, has an outside address ‘visible’ to the third-party carriers that transmit it to its intended location, and

v. Wolfe, 601 F.Supp.2d 441 (D. Conn. 2009) (looking at four factors and concluding that principal had reasonable expectation of privacy in her electronic mail files on her work computer despite policy allowing for routine monitoring because record did not indicate that was actually the practice of the school district to monitor users' accounts). But cf. United States v. Hart, No. 08-109-CR, 2009 WL 25552347, at *2 (W.D. Ky. Aug. 17, 2009) ("As further explained by the Magistrate Judge, the question of suppression of evidence that was provided by Yahoo!, but not found on the defendant's computer, hinges on whether law enforcement committed a constitutional violation of the Stored Communications Act. It did not. . . . Whether or not society is prepared to recognize as reasonable an expectation of privacy in all e-mail communications, the evidence in the record does not show that the defendant sought to preserve as private that which the plaintiff now seeks to introduce into evidence.").

At this point, a clarification of the court's finding that "the defendants had little to no control over Wyko's server" is appropriate. See [Doc. 88, pg. 12]. The Court based its finding on the fact that "Defendant Roberts testified that the server room was locked and that he did not have a key. Moreover, although he could designate some files from his computer to be saved to the server, he could not access all information on the server." [Doc. 88, pgs. 13]. The Court had earlier summarized the testimony as follows: "Defendant Roberts testified that Wyko's computer database was located in a locked room, to which he did not have a key. Persons who were not Wyko executives had to get permission from a manager to enter the room." [Doc. 88, pg.7]. What this summary of the testimony does not make clear is that Mr. Roberts was an executive in September 2007. In fact, he was the Director of Engineering at Wyko, and there were only two

also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not." Id. at *12 n.7.

other executives at his level. [Tr., pg. 7]. When discussing the I.T. room where the company's server was located, Mr. Roberts testified that the room had a lock on it and that he did not have a key; however, by way of explanation, Mr. Roberts testified that the production manager had the key, and he was an executive at the same level as Mr. Roberts within the company. [Tr., pg. 14-15]. Mr. Roberts then discussed his understanding of the privacy policy at Wyko with respect to e-mail which the Court accurately summarized as follows, "[Mr. Roberts] did not expect other employees, aside from his supervisors, to have access to his email. He kept copies of his email on his laptop computer, and these emails were also backed up on the server. He believed it to be company policy that no one could use the server to access someone else's email or information." [Doc. 88, pg. 6]. See also [Tr., pgs. 18-21, 27, 29]. Therefore, the privacy of e-mail and other documents on the server was not unlike that in Mancusi v. DeForte, 392 U.S. 364, 369-70 (1968).

The Report and Recommendation found "that the defendants could not be secure in the privacy of their email and other similarly situated files on the server," but the cases cited in support of the finding that Mr. Roberts does not have standing to challenge the seizure of such documents do not address analogous situations. [Doc. 88, pg. 13-14] (citing Guest v. Leis, 255 F.3d 325 (6th Cir. 2001); United States v. Costin, No. 3:05-CR-38, 2006 WL 2522377 (D. Conn. July 31, 2006)). For example, in Guest v. Leis, 255 F.3d 325 (6th Cir. 2001), after two "computer bulletin board systems" were seized, id. at 329-30, several users of the system filed a class action against the sheriff and his department. The first seized system was the Cincinnati Computer Connection Bulletin Board System (CCC BBS) which provided users with a password to send e-mails, participate in chat rooms, play games, or engage in "conferences" in which they could post or read messages on many topics, id. at 330; the second was the Spanish Inquisition

Bulletin Board System (SI BBS) which specifically included a posted disclaimer on privacy that notified users “that there are NO provisions for private messages on this board.” [Doc. 88 at 331]. The defendants argued that the plaintiffs did not have standing to assert Fourth Amendment claims. The Sixth Circuit quickly disposed of the SI BBS plaintiffs’ claim due to the disclaimer, then addressed the CCC BBS by first noting that its users “would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting” but then concluding that “[w]hether the users had more private material on the system that entitled them to standing is not a question we must reach since we conclude below that there was no Fourth Amendment violation in this case.” *Id.*; *see also id.* at 335 (“Plaintiffs also allege that defendants read their e-mail, an allegation defendants deny. . . . Plaintiffs’ assumptions are insufficient to establish a genuine issue of fact regarding an e-mail search.”). Similarly, in United States v. Costin, No. 3:05-CR-38, 2006 WL 2522377 (D. Conn. July 31, 2006), the other case which the Report and Recommendation said guided its finding, a similar issue was not factually before the court. In Costin, the government had conceded that the defendant had standing in order to avoid an evidentiary hearing. Additionally, unlike here, the defendant in Costin claimed an expectation of privacy “in all of the areas of the DataUSA office from which the government seized evidence,” *id.* at *5, even though he “failed to make a showing that he had access to, let alone control or possession of, the data stored on any of the computers aside from that located on his desk,” and even though his computer was not seized during the search.

If Hylton had access to and performed work on DataUSA computers other than that on his desk, he may have been able to show a privacy interest in the contents of such computers and their storage devices. However, he has not presented evidence that he had access to any such computers.

Id. at *6 n.6. Here, Mr. Roberts' laptop was seized; it was password protected, and it stored the documents he created as well as any e-mails in his account; Mr. Roberts does not claim a protected privacy interest in all materials on the server; and the copies of the documents and e-mails from his laptop were stored on the server, not broadcast or shared.

A more helpful case for the standing issue was cited in the Report and Recommendation as analogous support for contrary authority. [Doc. 88, pg. 13] (citing Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), reh'g denied, 554 F.3d 769 (9th Cir. 2009), cert. granted, City of Ontario v. Quon, No. 08-1472, 2009 WL 1513112 (U.S. Dec. 14, 2009)). In Quon, the Ninth Circuit held that a SWAT team member had a reasonable expectation of privacy in the content of text messages sent to and from his work-issued pager which were archived on Arch Wireless's server. The panel opinion held that the employee had a reasonable expectation of privacy in the messages even though (1) he was a government employee, (2) he had previously signed a no-privacy acknowledgment for internet and e-mail usage,⁴ (3) the pager was issued for SWAT-related duties, meaning that there was a likelihood that they would need to be reviewed based on the outcome of the emergency, (4) the text messages could fall under the definition of "public records" making them subject to an open records request,⁵ and (5) the

⁴ "The Department's general "Computer Usage, Internet and E-mail Policy" stated both that the use of computers "for personal benefit is a significant violation of City of Ontario Policy" and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Quon signed this Policy and attended a meeting in which it was made clear that the Policy also applied to use of the pagers. If that were all, this case would be analogous to the cases relied upon by the Appellees." Id. (citing Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir.2002); Bohach v. City of Reno, 932 F.Supp. 1232, 1234-35 (D.Nev.1996); O'Connor, 480 U.S. at 719; Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir.1987)).

⁵ "Appellees also point to the California Public Records Act ("CPRA") to argue that Quon had no reasonable expectation of privacy because, under that Act, "public records are open to inspection at all times ... and every person has a right to inspect any public record." . . .

messages were stored on the service provider's network. In Quon, the section of the opinion dealing with the Fourth Amendment candidly admitted that "[t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question," but then held that "users of text messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text messages stored on the service provider's network," tracing its reasoning to the U.S. Supreme Court's 1967 opinion in Katz v. United States, 389 U.S. 347 (1967), which held that

[L]istening to the conversation through the electronic device violated the user's reasonable expectation of privacy. *Id.* at 353. In so holding, the Court reasoned, "One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. **To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.**" *Id.* at 352. . . .

Id. Noting that the U.S. Supreme Court has treated pen registers differently, but explaining that the different was because "pen registers do not acquire the *contents* of communications." Id. (quoting Smith v. Maryland, 442 U.S. 735, 742 (1979)), the Quon court pointed out that the distinction between content and transmission information has long been recognized: "since 1878, . . . the Fourth Amendment's protection against 'unreasonable searches and seizures' protects a citizen against the warrantless opening of sealed letters and packages addressed to him in order to examine the contents." Id. (quoting United States v. Choate, 576 F.2d 165, 174 (9th Cir.1978), and (citing Ex parte Jackson, 96 U.S. 727 (1877)); United States v. Jacobsen, 466 U.S. 109, 114 (1984)). Based on the historically recognized distinction, the Quon court then turned to

Although the fact that a hypothetical member of the public may request Quon's text messages might slightly diminish his expectation of privacy in the messages, it does not make his belief in the privacy of the text messages objectively unreasonable. . . ." Id. at 905-08 (internal citations omitted).

is “Internet jurisprudence,” and highlighted a recent Ninth Circuit opinion in which the “outside-of-envelope rationale” was applied to hold that “e-mail ... users have no expectation of privacy in the to/from addresses of their messages ... because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.” Id. (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir.2008)). The opinion in Forrester, left open the issue of whether individuals have a reasonable expectation of privacy in the content of e-mails. Id. The Quon court then concluded:

We see no meaningful difference between the e-mails at issue in Forrester and the text messages at issue here. Both are sent from user to user via a service provider that stores the messages on its servers. Similarly, as in Forrester, we also see no meaningful distinction between text messages and letters. As with letters and e-mails, it is not reasonable to expect privacy in the information used to “address” a text message, such as the dialing of a phone number to send a message. However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider. Cf. United States v. Finley, 477 F.3d 250, 259 (5th Cir.2007) (holding that defendant had a reasonable expectation of privacy in the text messages on his cell phone, and that he consequently had standing to challenge the search). That Arch Wireless may have been able to access the contents of the messages for its own purposes is irrelevant. See United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir.2007) (holding that a student did not lose his reasonable expectation of privacy in information stored on his computer, despite a university policy that it could access his computer in limited circumstances while connected to the university's network); United States v. Ziegler, 474 F.3d 1184, 1189-90 (9th Cir.2007) (holding that an employee had a reasonable expectation of privacy in a computer in a locked office despite a company policy that computer usage would be monitored). . . .

Id. Importantly, the opinion in Quon does not purport to “endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-sensitive inquiry.” Id. Rather, the Ninth Circuit suggested, absent an agreement to the contrary, the plaintiffs had no reasonable expectation that the messages would remain private but that “[a]s a

matter of law,” the plaintiffs had a reasonable expectation that their employer would not review the messages “absent consent from either a sender or recipient of the text messages.” Id. The Ninth Circuit noted that the case would be analogous to other cases in which an employee’s expectation of privacy was unreasonable if its analysis were to be limited to looking at the computer policy signed by the employee in Quon which notified him that “[u]sers should have no expectation of privacy or confidentiality when using these resources,” rather than all circumstances surrounding the expectation of privacy; the difference in Quon turned on the fact that his employer followed an “informal policy” that the messages would not be audited if the overages were paid for, and it was therefore reasonable for the employee to have relied on the “operational reality” at the Department. As in Quon, the objective reasonableness of Mr. Roberts’ expectation of privacy in his e-mails was not diminished by the existence of backed-up copies on the server or by the fact that his supervisors could potentially ask to see his e-mail. The government did not introduce any privacy waivers or non-confidentiality warnings required of users of Wyko e-mail accounts and computers. Whether, as was mentioned at the hearing, Department of Justice employees have no expectation of privacy in what they do on their computers, [Tr., pgs. 32, 33-34, 35], is a separate question from the reasonableness of a Wyko employee’s expectation of privacy, because this is a fact-specific area of the law. See Convertino v. U.S. Dep’t of Justice, No. 04-CV-0236 (D.D.C. Dec. 10, 2009) [Doc. 167] (ruling that a DOJ employee’s use of his DOJ-provided e-mail address to communicate with his attorney did not cause him to waive the privilege of confidentiality under facts of case though the Department regularly accessed and saved e-mails, and finding that his expectation of privacy was reasonable) (citing O’Connor v. Ortega, 480 U.S. 709, 718 (1987) (“Given the great variety of work environments, . . . the question whether an employee has a reasonable expectation of

privacy must be addressed on a case-by-case basis.”)). For these reasons, Mr. Roberts objects to the finding that he does not have standing to challenge the seizure of documents and e-mails from Mr. Roberts’ computer which were saved to or backed-up on the server.

III. THE SEARCH WARRANT WAS NOT SUFFICIENTLY PARTICULAR.

Mr. Roberts’ motion to suppress was not limited to an argument about the forensic searching of the imaged hard drives.⁶ Mr. Roberts also suggested that the warrant was facially deficient, lacking particularity.⁷ In his motion to suppress, Mr. Roberts showed that the search warrant was insufficiently particularized because it provided no means by which officers executing the search could ascertain, from looking at a computer server or an individual computer, whether it was something to be seized without conducting a further and more particularized search of the contents of the computer data. [Doc. 40, pg. 2-7]. Mr. Roberts has argued that a warrant authorizing a search of a computer must specify with particularity the specific documents and files to be seized because if an investigator is allowed to open every file on a computer, claiming to be evaluating the files to see whether they relate to *evidence* of trade secret violations, then such unlimited access violates the Fourth Amendment’s prohibition against general warrants. *Id.* (citing United State v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (suppressing search of defendant’s computer where the warrant authorized search for evidence of

⁶ Compare [Doc. 88, pg. 2] (“Defendant Roberts contends [Doc. 39] that the search warrant was not sufficiently particular because it did not expressly narrow the search of the computer information. He also contends that the search of Wyko exceeded the scope of the search warrant.”) with [Doc. 61, pg., 4] (“The Search Warrant does not indicate how agents could have known which, if any, computers ‘contained evidence ‘of trade secret violations’”).

⁷ [Doc. 40, pg. 4] (“There is no way for an agent executing the warrant to ascertain, from looking at the computer server or individual computer, whether it is something to be seized without conducting a further and more particularized search of the contents of the computer data.”); [Doc. 40; pg. 9] (“[T]he warrant lacked both a limiting search methodology and a particularization of the places on the computer to be searched.”) [Doc. 61, pg. 10].

drug transactions and graphic files of child pornography were subsequently discovered, the court held that “law enforcement must engage in the intermediate step of sorting various types of documents then only search the ones specified in a warrant”), and discussing Gouled v. United States, 255 U.S. 298 (1921) overruled in part by Warden v. Hayden, 387 U.S. 294 (1967)).

The Report and Recommendation focuses its analysis on the search of the computers, but Mr. Roberts will address the seizure issue first.

Mr. Roberts objects to the court’s finding that “the affidavit in support of the search warrant provides probable cause for the seizure of both defendants’ computers,” [Doc. 88, pg. 17-18], because this finding does not respond to Mr. Roberts’ particularity argument which was based on the fact that *more* than these two computers were seized. As evidenced by the inventory, agents executing the warrant seized seven hard drives of data from six separately lettered rooms at Wyko. Even if the Report and Recommendation is correct that an e-mail included in the affidavit in support of the search warrant “establishe[d] that the defendants’ [two] computers were being used to disseminate and store information regarding the stolen trade secrets,” [Doc. 88, pg. 18], the Report and Recommendation does not provide a constitutional justification for seizing – not just searching – the massive quantity of data taken from Wyko or explain how officers executing the search could have known that these hard drives contained “evidence” of trade secret violations such as would differentiate this warrant from a general warrant prohibited by the Fourth Amendment. See [Doc. 40, pgs. 2-3] (“General warrants, which authorize searches without setting forth a particular description of the items to be seized, are expressly forbidden. See U.S. Const. amend IV; Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). The particularity requirement is met when the description particularly points to a definitely ascertainable place so as to exclude all others, and enables the officer to locate the

place to be searched with reasonable certainty without leaving it to his discretion. The less precise the description of the place to be searched or things to be seized, the less likely there is probable cause to seize the enumerated items. See Maryland v. Garrison, 480 U.S. 79, 84 (1987) (“By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications.”)).

Next, Mr. Roberts objects to the finding that the warrant was sufficiently particularized because “when the search warrant permits the agents to search a computer, they may search all of the files in that computer for the items to be seized.” [Doc. 88, pg. 20]. Further, to the extent that the Report and Recommendation relies on documents which were not incorporated to support its finding that the search warrant is sufficiently particular, Mr. Roberts objects. In United States v. Cioffi, No. 08-CR-415, 2009 WL 3738314 (E.D.N.Y. Nov. 2, 2009), a district court recently held that a warrant to search the defendant’s e-mail account was unconstitutionally broad, in part because the affidavit was neither attached nor incorporated into the warrant and therefore could not be used to particularize the warrant. Id. at *7 (“The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.”) (quoting Groh v. Ramirez, 540 U.S. 551, 557 (2004)).

Magistrate Judge Pollak signed the Warrant, which authorized a search of “the premises known and described as electronic mail address ‘matt.tannin@gmail.com’.” The Warrant contained a boilerplate statement reflecting the magistrate judge’s “satisf[action] that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property ... described is now concealed on the ... premises above-described and establish grounds for the issuance of this warrant.” **The government concedes, however, that the Affidavit was not attached to or incorporated by reference into the Warrant. . . .**

Attachment A also set forth procedures for obtaining the account from Google. It directed Google employees to “locate, isolate, and create an exact duplicate” of all records sought, and to produce the duplicate to the executing officer “in electronic form.” **The attachment did not, however, describe any procedures for the executing officer to follow in searching the account and seizing particular records.**

Id. at *2 (emphasis added). Here, the warrant to search Wyko expressly incorporated Attachments A and B, but appears not to have incorporated the application and affidavit for the search warrant. The affidavit, not the attachments, contained the “two and one-half page section entitled Specifics of Search and Seizure of Computer Systems” which the Report and Recommendation noted in the section finding the warrant sufficiently particular [Doc. 88, pg. 19] and mentioned in the section finding the scope of the search reasonable [Doc. 88, pg. 25].

The finding that an agent may search all files within a computer writes the particularity requirement out of the Fourth Amendment and gives forensic examiners the power to search a computer independent from the probable cause established in the warrant. The Report and Recommendation found that “agents properly seized the defendants’ computers and searched all the files therein for the items listed in . . . the search warrant” [Doc. 88, pg. 22] and that “a search of all the files on the defendants’ computers and on Wyko’s servers for the items listed in Attachment B was reasonable,” [Doc. 88, pg. 35], at least in part based on the court’s rejection of Mr. Roberts’ argument that each file on a computer is a separate container and that probable cause did not exist to search every container, reasoning:

When executing a search warrant, officers are permitted to look in any container or location on the premises that could hold the items to be seized, even if those containers are not specified in the search warrant. As the Supreme Court noted with regard to searches for documents, the executing agent may examine some “innocuous” items “at least cursorily, in order to determine whether they are, in fact, among those [items] authorized to be seized.”

[Doc. 88, pg. 19-20] (internal citations omitted). The common law-based necessity of analogizing from more familiar subjects of Fourth Amendment inquiry to computers should not override the fact that computers are unique. See United States v. Burgess, 576 F.3d 1078, 1088-89 (10th Cir. 2009) (“[A]nalogies to closed containers or file cabinets may lead courts to ‘oversimplify a complex area of Fourth Amendment doctrine and ignore the realities of massive modern computer storage.’”) (quoting United States v. Carey, 172 F.3d 1268, 1275 (10th Cir.1999) (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994))). Cf. United States v. Andrus, 482 F.3d 711, 718 (10th Cir. 2007) (noting that courts have “attempted to analogize computers to other items more commonly seen in Fourth Amendment jurisprudence” to determine privacy interests but quoting article which pointed out that “[C]omputers are playing an ever greater role in daily life and are recording a growing proportion of it.... [T]hey are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.... Each new software application means another aspect of our lives monitored and recorded by our computers.”) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L.Rev. 531, 569 (2005)).

Next, Mr. Roberts objects to the Court’s observation that “search warrants are typically concerned with what items may be seized, i.e., what the officers are searching for, rather than the method in which the officers execute the search” both insofar as the Court is characterizing Mr. Roberts’ position as being only concerned with methodology of a forensic examination⁸ and

⁸ Although Mr. Roberts’ argument about particularity is not limited to the manner in which the search was conducted, that was an aspect of it raised in his motion. See [Doc. 40, pg. 7]; see also In re Search of 3817 W. West End, First Floor Chicago, Illinois, 60621, 321 F. Supp. 2d 953 (N.D. Ill. 2004) (magistrate judge refused to issue a warrant without a search protocol settled beforehand); United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930 (D. Utah Apr. 12,

insofar as the statement minimizes the constitutional reasonableness requirement for the execution of warrants. Mr. Roberts' suggestion that a computer examination can be conducted in accordance with the limitations of the search warrant is not necessarily a suggestion as to the examiner's methodology. Rather, it is a constitutional imperative that a search must be conducted in accordance with limitations established in the warrant. See United States v. Wecht, 619 F.Supp.2d 213 (W.D. Pa. 2009). In Wecht, the government argued "that, as a practical matter, once it is granted authorization to access a computer, it has the right to examine every file in order to find evidence that is relevant to the supporting affidavit," and the court noted that such an "argument appears to be a reference to cases recognizing the principle that the Government need not accept the user's own file designations at face value, since incriminating evidence can easily be stored under an innocuous file name, and the Government therefore has the right to use appropriate search mechanisms in order to locate relevant evidence, even if it involves looking beneath the facade of an apparently innocuous document." Id. The opinion continued as follows:

However, the important point is that, while the Government may choose its own preferred search mechanism for obtaining relevant evidence, the search of computer files must be conducted *in accordance with limitations established in the warrant*.

Moreover, the fact that the Government may have the right to conduct a controlled *search* of an entire computer base for incriminating evidence is a concept distinct from the idea that the Government may automatically *seize* every piece of data stored on the computer. Cases have recognized, for example, that when a law enforcement officer searching a computer for evidence of a particular type of crime inadvertently discovers evidence of other crimes, that officer must obtain a second search warrant in order to continue searching for evidence of the second crime.

2001) (suppressing evidence in absence of search protocol) ("[M]ethods or criteria should have been presented to the magistrate before the issuance of the warrants or to support the issuance of a second, more specific warrant once intermingled documents were discovered.").

Wecht, 619 F.Supp.2d at 245-46 (internal citations omitted).

The Report and Recommendation characterizes the defense's argument this way: "The defendants contend that even if the seizure of the computers and their offsite searches were proper, the agents could not search every file on the computers for evidence of theft of trade secrets. They liken each file on a computer to a separate container and argue that no probable cause exists to search every container." [Doc. 88, pg. 19]. It is a correct statement of the law that officers executing a search warrant "are permitted to look in any container or location on the premises that could hold the items to be seized, even if those containers are not specified in the search warrant." [Doc. 88, pg. 20]. However, any potentially irrelevant files must be related to the probable cause which formed the basis for the issuance of a search warrant. Mr. Roberts more fully discussed this in his Reply to the Government's Response to his Motion to Suppress: as understood by the U.S. Supreme Court, the "prohibition against general searches and general warrants serves primarily as a protection against unjustified intrusions on privacy," meaning that

[e]ven if the item is a container, its seizure does not compromise the interest in preserving the privacy of its contents because it may only be opened pursuant to either a search warrant, see *Smith v. Ohio*, 494 U.S. 541 (1990); *United States v. Place*, 462 U.S. 696, 701 (1983); *Arkansas v. Sanders*, 442 U.S. 753 (1979); *United States v. Chadwick*, 433 U.S. 1 (1977); *United States v. Van Leeuwen*, 397 U.S. 249 (1970); *Ex parte Jackson*, 96 U.S. 727, 733 (1878), or one of the well-delineated exceptions to the warrant requirement. See *Colorado v. Bertine*, 479 U.S. 367 (1987); *United States v. Ross*, 456 U.S. 798 (1982)."

Horton v. California, 496 U.S. 128, 141, 142 n.11 (1990) (emphasis added).

The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found. . . . Probable cause to believe that a container placed in the

trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.

Id. at 140-41 (quoting United States v. Ross, 456 U.S. 798, 824 (1982)). Like the automobile/trunk analogy, the computer/file distinction matters for the probable cause analysis in determining whether, even if the government had probable cause to search parts of the computers seized from Wyko, it lacked probable cause to search other parts. The government may not employ an electronic device (like computer forensic software) to obtain information in an area where one has a reasonable expectation of privacy that could not be gained through sensory observation. See United States v. Karo, 468 U.S. 705, 715 (1984); United States v. Knotts, 460 U.S. 276 (1983). Without probable cause to search the entire contents of each computer, the government cannot rely on an “electronic device” to circumvent the warrant requirement.

Therefore, unless probable cause is found to be coextensive with the entirety of a computer’s contents, the search of the entirety of a computer’s contents cannot be justified by the finding of probable cause to search for particular items and violates the Fourth Amendment to the U.S. Constitution. For example, when there is probable cause to search for images, only those filename extensions associated with image files should be allowed to be searched; when certain topics are the subject of the investigation, a search of the whole computer could be run by a forensic program that returns potentially matching items such that any irrelevant and non-probative files viewed by a human analyst are at least related to the probable cause; or the metadata associated with a given file showing when it was created or modified could limit which files are searched. Here, the warrant issued based on probable cause to seize the items listed in Attachment B which, as summarized by the court, permitted the seizure of many types of items, including photographs and correspondence. [Doc. 88, pg. 15-16].

The Report and Recommendation quotes from United States v. Ogden, No. 06-20033-STA, 2008 WL 4982756, at *4 (W.D. Tenn. Nov. 18, 2008), in which the district court held that since the file names would not necessarily “openly and obviously denote child pornography. . . . a searching agent must reasonably access these and other files for the purpose of determining whether they contain the child pornography described in the warrant affidavit.” [Doc. 88, pg. 20; see also pg. 21, discussing United States v. Tillotson, No. 2:08-CR-33, 2008 WL 5140773 (E.D. Tenn. Dec. 2, 2008)]. Respectfully, one cannot analogize the situation that exists with searching computer files for child pornography with a search of business records in electronic format. Child pornography is, in and of itself, contraband. In this case, the warrant’s command to seize items, in electronic or other format, having to do with theft of trade secrets, does not call for the search and seizure of items that would constitute contraband in and of itself, but instead allows for the examination and seizure of material that would provide some evidence of a violation of the Economic Espionage Act. The type of lawful search and seizure conducted is dependent upon the probable cause to search for a specific type of evidence, the nature of the evidence sought, and the manner of its storage. Cf. Berger v. United States, 388 U.S. 41 (1967) (“[The two affidavits] might be enough to satisfy the standards of the Fourth Amendment for a conventional search or arrest. But I think it was constitutionally insufficient to constitute probable cause to justify an intrusion of the scope and duration that was permitted in this case.”) (Stewart, J., concurring) (internal citation omitted); Couch v. United States, 409 U.S. 322, 349 n.6 (1973) (Marshall, J., dissenting) (“I recognize that there is an alternate view However, this Court has held that increasingly severe standards of probable cause are necessary to justify increasingly intrusive searches.”) (citing Camara v. Municipal Court, of City and County of San Francisco, 387 U.S. 523 (1967); Terry v. Ohio, 392 U.S. 1 (1968); Stanford v. Texas, 379 U.S.

476 (1965)). In the child pornography context, the nature of the evidence is that it is contraband. As the cases discussed in the Report and Recommendation demonstrate, child pornography may be pervasive throughout electronic media, intentionally hidden from others through the use of false filenames or file extensions, and buried by the user of the contraband into various folders or subfolders in an effort to subvert any third party, particularly law enforcement, from finding the contraband. See United States v. Ogden, No. 06-20033-STA, 2008 WL 4982756, at *3 (W.D. Tenn. Nov. 18, 2008). In that context, some courts have held that given the nature of the evidence sought – child pornography – a search and seizure involving the taking of the entire computer hard drive, or an imaging of the entire hard drive, coupled with a search of the entirety of the contents, was reasonable in order to look for child pornography. In this case, the type of evidence sought was not, in and of itself, contraband, and specific facts must exist to support the nature of the search conducted and its reasonableness under the Fourth Amendment. No such facts, particular and specific to this case, were alleged to support such a broad seizure and search of all server and workstation hard drives from Wyko.

IV. THE EXECUTION OF THE SEARCH WARRANT EXCEEDED ITS SCOPE.

Mr. Roberts objects to the Court's finding that "[b]ecause the extent of the search was proper, the Court also generally finds a search of all the data on the computers for the items in Attachment B was reasonable, does not exceed the scope of the search warrant, and does not convert the search warrant into a general warrant, even without any limiting methodology in place. [Doc. 88, pg. 23]. For the reasons discussed in the previous section, Mr. Roberts' argument was not limited to the manner in which the computers were searched. When multiple hard drives' worth of data were seized without having shown a nexus between those computers

and the alleged crime, the agents executing the warrant exceeded the scope of authority it granted.

The affidavit must demonstrate “that there is reasonable cause to believe that the specific ‘things’ to be searched for and seized are located on the property to which entry is sought,” not just “that the owner of property is suspected of a crime.” Zurcher v. Stanford Daily, 436 U.S. 547, 556 (1978). Particularly, “facts providing a nexus between the crime and the . . . [location] to be searched are a critical element that must be included in the affidavit.” State v. Longstreet, 619 S.W.2d 97, 99 (Tenn. 1981) (citing Whiteley v. Warden, 401 U.S. 560, 565-66 (1971)). Cf. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004 (9th Cir. 2009) (“[A case from 1982] involved a few dozen boxes and was considered a broad seizure; but even inexpensive electronic storage media today can store the equivalent of millions of pages of information.”); United States v. Mitchell, 565 F.3d 1347 (11th Cir. 2009) (“Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives.”); United States v. Hodson, 543 F.3d 286 (6th Cir. 2008) (Batchelder, J) (reversing the district court’s denial of the defendant’s motion to suppress and vacating defendant’s conviction for possession of child pornography because “it was unreasonable for the officer executing the warrant in this case to believe that probable cause existed to search Hodson’s computers for child pornography based solely on a suspicion-albeit a suspicion triggered by Hodson’s computer use-that Hodson had engaged in child molestation”).

Mr. Roberts also objects to the finding that “the ten-day limitation on the execution of a search warrant applies to the seizure of the computers or, alternatively, to the imaging of their contents.” [Doc. 88, pg. 25]. Mr. Roberts objects to the Report and Recommendation’s reliance

on an amendment to Rule 41 of the Federal Rules of Criminal Procedure which was not in effect when the computers were seized in this case. Rule 41 is clear that a search warrant must be executed within ten days, Fed. R. Crim. P. 41 (e)(2); the warrant commanded the search to be accomplished within ten days. The “practical challenges inherent in analyzing electronically stored data” [Doc. 88, pg. 27] should not excuse non-compliance. Cf. Melendez-Diaz v. Massachusetts, 129 S.Ct. 2527 (2009) (“[R]espondent asks us to relax the requirements of the Confrontation Clause to accommodate the ““necessities of trial and the adversary process.”” It is not clear whence we would derive the authority to do so. . . . The Confrontation Clause-like those other constitutional provisions-is binding, and we may not disregard it at our convenience.”). If more time had been needed, the agents could have requested an extension of time or sought another warrant.

V. THE APPROPRIATE REMEDY IS SUPPRESSION OF THE EVIDENCE SEIZED.

The doctrine of severance sometimes permits courts to suppress only the evidence seized pursuant to the invalid portions of a warrant while admitting evidence seized based on any valid, separable parts of the warrant, see United States v. Ford, 184 F.3d 566, 579 (6th Cir. 1999), but when a lack of particularity is characteristic of an entire warrant, suppression of all seized materials is the proper remedy. See e.g., United States v. Wecht, 619 F.Supp.2d 213 (W.D. Pa. 2009) (“Because the Laptop Warrant's description of items to be seized was so patently overbroad as to fail, on its face, to particularize the items to be seized, any reliance on that warrant was objectively unreasonable and the evidence obtained as a result of that search must be suppressed.”).

Here, even though the warrant issued based on probable cause, as was set forth in the affidavit, the warrant was not sufficiently particular so as to limit the executing officers’

discretion when executing the warrant. One purpose of the Fourth Amendment's particularity requirement is to prevent the "general, exploratory rummaging in a person's belongings." Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). As pointed out in Groh v. Ramirez, in support of its finding that the good faith exception could not have the deficient warrant, "[g]iven that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid" 540 U.S. 551, 557 (2004). In Groh, the warrant did not describe the items to be seized at all, although the application adequately did, the items to be seized were orally described to the executing officers, and the search did not exceed the limits intended by the magistrate. Id. 540 U.S. at 557-58. Here, Attachment B to the warrant to search Wyko listed eight categories of items to be seized, but this list was broad and included authority to seize "[c]omputers, computer hardware, software, computer related documentation, [and] passwords . . . which contain evidence related to violations of Title 18, United States Code, Sections 1832 and 2314 as described more fully in paragraphs (3) through seven (7) below." See [Doc. 88, pg. 15]. Paragraphs three through seven are summarized in the Report and Recommendation. Id. According to the inventory, many hard drives were imaged for off-site review. Given the amount of data on the server and computers which were imaged and the lack of guidance included in the warrant to enable officers (1) to identify which computers "contained evidence" related to the violation and (2) to prevent general, exploratory rummaging, the whole warrant is overbroad, and no evidence can be admitted against Mr. Roberts under the doctrine of severance.

VI. CONCLUSION

An evidentiary hearing was held before the Magistrate Judge on the defendant's motion to suppress on November 12, 2009. The defendant briefed the suppression issues for the Court

prior to the evidentiary hearing, and the defendant further relies upon, and expressly incorporates herein by reference, his motion to suppress [Doc. 39], supporting memorandum [Doc. 40], and reply [Doc. 61]. Additionally, defendant relies upon the testimony and exhibits presented at the evidentiary hearing, as well as the arguments of counsel.

Respectfully submitted this 4th day of January, 2010.

s/ W. Thomas Dillard
W. THOMAS DILLARD
[BPR # 002020]

s/ Stephen Ross Johnson
STEPHEN ROSS JOHNSON
[BPR# 022140]

ITCHIE, DILLARD, & DAVIES, P.C.
606 W. Main Street, Suite 300
P. O. Box 1126
Knoxville, TN 37901-1126
(865) 637-0661
www.rddlafirm.com
Counsel for Clark Alan Roberts

CERTIFICATE OF SERVICE

I hereby certify that on January 4, 2010, a copy of the foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic receipt. All other parties will be served by regular U.S. mail. Parties may access this filing through the Court's electronic filing system.

s/ Stephen Ross Johnson